Request for Access to Blocked Internet Content

Instructions for completing the NIH Request for Access to Blocked Internet Content

Please provide justification for access to the blocked Internet site or category by specifying how it applies to your job in support of NIH.

Web sites categories based on Internet content are blocked by the NIH Incident Response Team (IRT) in accordance with HHS and NIH standards and policy.

Requesting access to blocked Internet content using the appropriate NIH form completely and accurately is evaluated to ensure sufficient justification is provided as an exception to the HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications and the NIH policy on Limited Authorized Personal Use of NIH Information Technology (IT) Resources.

The Request for Access to Blocked Internet Content form consists of five (5) pages with annual renewal required since access, if granted, is only for one year from the date of final approval.

Page 1: The requesting user must provide all information on the first page under "Access Acknowledgment" except for IP address that the IC ISSO will later provide.

Page 2 requires providing justification in sufficient detail for a full evaluation of the request for final approval. Attachment of additional pages is recommended to fully describe the business/mission case for consideration. The requesting user's supervisor must provide their approval/disapproval of the request and requested information.

Page 3 requires review and approval/disapproval by the IC Information Systems Security Officer (ISSO), including listing compensating security controls in place to safeguard the system, user and data from any additional risks associated with access to blocked Internet categories and sites. The IC Chief Information Officer (CIO) determines approval/disapproval to ensure compensating security controls are adequate to protect NIH IT resources based on mitigated risks described in the certification and accreditation standards and plans established to safeguard resources as evaluated by the HHS Office of the Inspector General (OIG) during audits and related reviews.

Page 4 requires review and approval/disapproval by the IC Executive Officer (EO) that the request justification is deemed appropriate and necessary in the conduct of official government business in accordance with NIH and HHS policies and procedures. If approved by the IC Executive Officer, then the IC ISSO assigns a static (Internet Protocol) IP address as a compensating security control to the request for submission to the NIH Office of the Director (OD) staff to review and final approval by the NIH Chief Information Security Officer (CISO).

Page 5 requires listing and signature of the requesting user(s) at the time of submission of the form. After approval by the IC Executive Officer, the IC ISSO will add the IP address to the form prior to submission for final approval.

Overall, the IC ISSO oversees the request process upon receipt of the request to ensure its completion for final approval or notification to the requesting user the reason for disapproval.

Instructions for completing the NIH Request for Access to Blocked Internet Content (Web 2.0)

Please provide justification for access to the blocked Internet social media websites by specifying how it applies to your job in support of NIH.

Web sites based on Internet content are blocked by the NIH Incident Response Team (IRT) in accordance with HHS and NIH standards and policy.

The Request for Access to Blocked Internet Content (Web 2.0) form consists of three (3) pages.

Page 1: The requesting user must provide all information on the first page under "Access Acknowledgment" except for IP address that the IC ISSO will later provide. Provide justification in sufficient detail for a full evaluation of the request for final approval. Attachment of additional pages is recommended to fully describe the business/mission case for consideration.

Page 2 requires the requesting user's supervisor provide their approval/disapproval of the request and requested information. The request requires review and approval/disapproval by the IC Information Systems Security Officer (ISSO), including listing compensating security controls in place to safeguard the system, user and data from any additional risks associated with access to blocked Internet categories and sites. The review determines that compensating security controls are adequate to protect NIH IT resources based on mitigated risks described in HHS and NIH standards and plans established to safeguard resources as evaluated by the HHS Office of the Inspector General (OIG) during audits and related reviews. The review also ensures that the request justification is deemed appropriate and necessary in the conduct of official government business in accordance with NIH and HHS policies and procedures.

If approved, then the IC ISSO assigns a static (Internet Protocol) IP address as a compensating security control to the request for submission to the NIH Office of the Director (OD) staff to review and final approval by the NIH Chief Information Security Officer (CISO).

Page 3 requires listing and signature of the requesting user(s) at the time of submission of the form. The IC ISSO will add the IP address to the form prior to submission for final approval.

Overall, the IC ISSO oversees the request process upon receipt of the request to ensure its completion for final approval or notification to the requesting user the reason for disapproval.